PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 12/14 — A1

(11) International Publication Number: WO 97/44736

(43) International Publication Date: 27 November 1997 (27.11.97)

(21) International Application Number: PCT/US97/08264

(22) International Filing Date: 15 May 1997 (15.05.97)

(30) Priority Data:
08/652,862 23 May 1996 (23.05.96) US

(71) Applicant: APPLE COMPUTER, INC. [US/US]; 1 Infinite Loop - MS: 38-PAT, Cupertino, CA 95014 (US).

(72) Inventor: WEHRENBERG, Paul, J.; 3516 Ross Road, Palo Alto, CA 94303 (US).

(74) Agents: CARMICHAEL, Paul, D. et al.; Apple Computer, Inc., 1 Infinite Loop - MS: 38-PAT, Cupertino, CA 95014 (US).

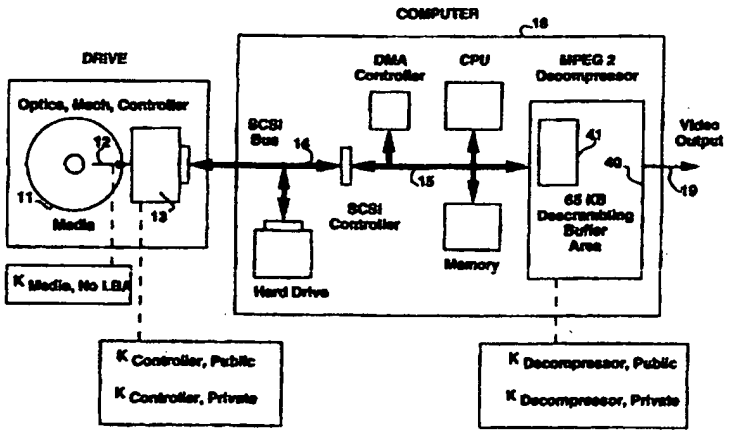
(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ARIPO patent (GH, KE, LS, MW, SD, SZ, UG), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published

With international search report.

Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: METHOD AND APPARATUS FOR TWO-LEVEL COPY PROTECTION



(57) Abstract

An apparatus and method for providing two levels of copy protection, including a first method for copy protection, including a key, and a second method for copy protection. One level of copy protection is a moderately secure level to allow decrypting a medium- to high-bandwidth data stream without significant delay of the data stream. The second level of copy protection can be highly secure but can be utilized less often and so can be decrypted more slowly. One useful combination is to use a key encryption scheme for the first level of copy protection of a primary data stream, then to use the second protection scheme to securely transfer the first level key from a protected storage location to a decoding location. Encoded primary data can be stored on a removable media, together with the decryption key stored in a special location. The media drive unit can access the special location and, using the second level copy protection scheme, transfer the key securely to a descrambling unit. The first level copy protection can involve selective reordering of data subunits within a data unit according to a scrambling vector, then encoding the scrambling vector using the first key, and storing the encoded scrambling vector with the corresponding data unit.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

METHOD AND APPARATUS FOR TWO-LEVEL COPY PROTECTION

Field of the Invention

This invention relates to data encryption and decryption, and more particularly to an improved method and apparatus for using one level of encryption to establish a secure communication channel, then passing a decryption key over that channel for subsequent decryption. This invention includes a new method of scrambling bulk data. This invention is particularly useful for protecting bulk information intended for widespread distribution such as movies or music in CD or DVD formats.

Background of the Invention

The field of data encryption has been the subject of extensive scholarly investigation and has been the topic of many patents in the United States and other countries. For general reference, the background description in each of United States Patent Nos. 5,497,422 (Tysen et al., 5 March 1996) and 5,438,622 (Normile et al., 1 August 1995) discuss representative encryption schemes known in the art. Each of these patent applications are assigned to Apple Computer, Inc. These patents are incorporated herein by reference in their entirety.

A wide variety of information is sold to consumers in various forms. One major category of information is computer software. Another major category of information is music, often in the form of CDs or tape. Still another major category of information is movies, usually over cable or satellite television links but often in the form of analog tape or LaserDisc. There is a tension in distribution of any form of information because if consumers will buy it from a rightful owner, other consumers are likely to buy illegal copies made from legitimate originals.

Various copy protection schemes have been considered for use with various media. Scrambling of cable or satellite channels is common. A variety of anti-copying schemes are used in analog video tape. CDs or digital tape can be encoded with anti-copying codes.

Distribution of various information in digital form has troubled many content providers because making the information available potentially makes it quite simple for a user to make one or many illegal copies of that content. Forms of such content include movies, music, and data such as encyclopedic

compilations. This issue has been widely discussed in relation to audio CDs, LaserDiscs and other formats.

In the personal computer environment, the protection of intellectual property has been of interest since the beginning of the industry. In computer software, a variety of special encoding or encryption schemes have been used. Some software requires a hardware key to be connected in some way to the computer system. Use of such systems frustrates casual copiers but often has some negative impact on legitimate users.

Due to the rapid growth of the industry and the technical difficulties associated with controlling information flow in an intrinsically open architecture, the industry players have more often than not written the problem off as intractable, at least in relevant time and cost frames. However, the problem remains. And as the convergence between entertainment and computing moves forward, driven by the evolution of hardware and software technologies, industry participants with different attitudes and requirements enter the discussion.

The problem is particularly acute with the advent of the DVD technology as a mass storage device in computers. DVD is a new, high density storage medium capable of storing about 4.5 through 18 gigabytes of information on a single 12 centimeter disc. Commercial products have already been announced before May 1996 for availability before December 1996.

The movie industry, with its high degree of sensitivity to intellectual property protection, is concerned that none of the new transmission modalities, including personal computers, enable free copying of their material. Other content providers have similar concerns. Some sort of copy protection scheme would encourage content providers, such as the movie industry, to distribute information such as movies in digital format.

The proposed protection scheme is intended to fall between a "screen door latch" (too weak) and a "Fort Knox" approach (too clumsy and expensive for mass-market products). Although it will be discussed here in the context of DVD, one skilled in the art will appreciate that this copy protection scheme can be used in many other situations or collections of elements.

Summary of the Invention

The invention provides a two-stage copy protection scheme. This is particularly useful where large quantities of data are to be encrypted and decrypted using an encryption key but that encryption key is to be carefully protected until the data is to be decrypted using an authorized retrieval system.

One stage of the retrieval system includes an encryption scheme to assure that the retrieval is made in an authorized system, and another stage of the retrieval system uses a stored encryption key to decode the data of interest. In one preferred implementation, the encryption key is used as a descrambling code.

To minimize the performance impact on the apparatus and not constrain use of system resources by low priority or low value data streams, the information flow can be broken into elements with a distinct hierarchy of bandwidth. For example, an MPEG stream (high bandwidth) may be merely scrambled, the scrambling control bits (much lower bandwidth) may be encoded, and only the MPEG-decode key information necessary to decode the scrambling control bits (very low bandwidth) is key encrypted.

The scrambling can be done in any of many ways, some of which are discussed in detail below. For example, the order of the data within a unit of data can be reordered in a controlled way to give a scrambled signal. Each unit of data, such as a 64 KB block, can be scrambled in a defined way, then a descriptor which characterizes that scrambling can be encrypted using a key and the encoded descriptor can be stored with the relevant block of data. A single key can be used to decrypt any scrambling descriptor and the descriptor can be changed for each unit of data, that is, each unit of data can be independently scrambled. With a key available, it is relatively straightforward to correctly reorder the scrambled data into the original, "clear text" format. With no key, if a sufficiently complex scrambling method has been chosen, it can be challenging to identify the correct key by trial and error, particularly since each data unit is scrambled in a different pattern. With the key, a moderately complex scrambling method will not have a significant effect on data reconstruction rate and thus becomes transparent to the user.

This copy protection becomes much more powerful if the key can be changed for different units of primary information, for example for each movie title.

Storage and access to this key raises an interesting challenge, but this can be managed very conveniently by using a separate encryption mode to secure the key and provide it in a coordinated fashion with the program of interest. One way to do this is to store the key in a secure manner on the same storage medium as the scrambled information. The mechanism of this separate storage mode can be set at a desired level of complexity. One preferred mode is to make this key inaccessible by typical access operations, but readily accessible through special operations. Specifically, in just one preferred embodiment, the

key may be stored at a location which is inaccessible to a host computer which can only access a logical block address, but readily accessible to a drive control unit, which may be designed to access a specific physical address, preferably not a logical block address. This access capability can be designed into the drive control unit, and the relevant key can be stored at the corresponding location when the media is prepared.

Subsequent manipulation of the key can be under close security. Since the key need be extracted only once, taking even several seconds to extract and/or transfer the key will not have a significant impact on the user.

In one preferred embodiment, a public/private key pair is stored in a disk drive mechanism and a second public/private key pair is stored in a decryption/decode unit such as an MPEG2 decoder. The key pairs are used to establish a secure channel of communication between the disk drive and the decoder and, once the channel is secure, a message can be read safely from the storage medium into the decoder even if the data path for the channel between these elements is unsecure. This message is the information content or message protected using the high-level security scheme, but is itself the key for the low-level security scheme. Passing this encrypted key over a secure channel makes it extremely difficult to intercept the key and use it for improper purposes.

This inhibits casual copying by setting up the system so that the data flow path between a source, such as a DVD-ROM drive, and a destination, such as an MPEG decoder carries only scrambled information and decryption to clear text occurs only in an isolated portion of the system, preferably within a special descrambler/decoder unit. The scheme cannot be defeated except by system patches, and a new patch is required for each title defeated, that is for each new title encryption key.

Scrambling and encrypting the primary information means that a read of the media by a system that does not implement correct decoding will give unintelligible results. Only the application software, with a little help from the operating system, can allow correct decoding of the primary information, as in correct decoding and display of a movie.

Distributing the copy protection elements balances the economic and processing power burden so that no single part of the overall system bears all the cost and effort of protecting the valuable information. Modifying the media format to carry scrambled data and modifying the drive to take advantage of its closed sub-system status balances these costs.

Moving the implementation burden on the computer system toward the peripheries, i.e. the media, the mass storage device, and the application software minimizes the impact on the operating system software and motherboard hardware. This method and apparatus avoids the need to create new high bandwidth information flow paths and new file systems while providing useful protection for the valuable source information.

One object of this invention is to provide reasonably effective prevention of casual copying by a user.

Another object of this invention is to provide a copy protection scheme with little or no impact on or modification of the traditional, primary computer components.

Still another object of this invention is to minimize the performance impact of the protection scheme by selectively protecting the most unique or most valuable portions of a data stream.

This and other objects and advantages of the invention, as well as the details of an illustrative embodiment, will be more fully understood from the following specification and drawings.

Brief Description of the Drawings

Figure 1 illustrates an apparatus useful in practicing this invention.

Figures 2A, 2B and 2C illustrate a source data structure in its original form (2A), then formatted and addressed after scrambling (2B) and then formatted and addressed after encrypting the scrambling vector (2C).

Figure 3 illustrates encryption of a 32 element scrambling vector.

Figure 4 illustrates descrambling inside an MPEG2 decoder.

Description of the Preferred Embodiments

Representative elements and the process of a preferred implementation of the copy protection scheme are described below. A preferred embodiment will be described by way of example. Figure 1 gives a schematic of the complete system. Note that the MPEG decoder is depicted as a hardware element, but the copy protection method can be used, perhaps with a lesser degree of protection, when the MPEG decoder is a software process. A more generic system includes only a medium, a reader for that medium, a destination for information from that medium, and a channel between the reader and the destination.

The medium does not need to be physically close to the destination. For example, the source information might be stored on a server such as a video-

on-demand server, and the destination might be located many miles away, as in a set top box, cable decoder, or other interface. For example, the server might include a reader which securely transfers a decryption key to the destination in a user's home, then communicates a scrambled data stream over some channel to the destination where it is descrambled according to the decryption key.

The channel for communicating the decryption key need not be the same as the channel for communicating the encoded, bulk information, but a single channel might be used for both purposes. A channel might be a data path through a computer but might also be a telephonic, television cable or satellite link or even a combination of two or more such links. The decoding can be done after any number of intervening transfers of the encoded digital information. One useful example would be a decoder coupled directly to a television set for direct and secure transmission of an encoded movie from a source to an end user.

The channel can include several connected data paths and still safely transfer encoded information. For example, the primary information may be stored in encoded form on a server. That server might be connectable through several separate links, perhaps telephone or cable switching boxes, until final delivery to a decoder.

One encoding scheme is used to encode the primary data. A key for this scheme is maintained according to one or more of a variety of methods. A second encoding scheme is used to transfer the key from a secure location to a location for use in decoding the primary data. In a preferred embodiment, the key for the primary data is stored with the data in a generally inaccessible location. This might be in a special track or location on a disk containing the primary information. Alternatively, this might be maintained on a server as in, for example, a video-on-demand system, or in a selected-access system as in, for example, a pay-per-view system.

The specific encoding scheme for the primary information may take any of a variety of forms. Some encoding schemes are known in the art but there are other, new schemes that are particularly useful. One particularly useful scheme is a simple scrambling scheme where the scrambling key is sufficiently complex to make brute-force decoding difficult, but simple enough to allow for rapid decryption when the correct key is available. The encoding scheme for the secondary information, here the scrambling or primary information key itself, also may take any of a variety of forms. In one preferred form, this secondary encoding uses two pairs of private and public keys to establish a

secure channel between the reader, for example the device where the primary key is maintained, and the destination, for example the device where the primary key is to be used.

As illustrated in Figure 1, there are five keys involved in one preferred implementation of the copy protection apparatus of this invention, one for the primary information and four for secure transfer of that key.

Secure Transfer of the Primary Information Key

In one preferred embodiment, the primary information key is placed on the media during manufacture. It may be stored in a location or sub channel that is readily accessible to the drive controller but difficult or impossible to access otherwise. In a preferred embodiment, is not in an area that is addressable by logical block address (LBA) and thus is not accessible by devices other than the drive controller itself. This primary information key is transferred as the message for a public key/private key transaction through the open computer system to a descrambler where it is used to descramble the primary information.

The drive controller is possessed of a public key and a private key, and has the capability of receiving another entity's public key. The drive can then encrypt a message using its private key and the received public key. This encrypted message can be requested by the operating system and passed to the owner of the non-drive public key, the destination.

The non-drive entity can then use its own private key and the drive's public key to decrypt the received message. As noted above, the key on the media is the message for the second encoding system. Thus the key for the primary encoding is itself encoded using the second encoding system and transferred through the open computer system to the non-drive entity, where it is decoded according to the second encoding scheme. This key can then be loaded into the primary decoding system and used directly.

The key encoding transaction described above uses very robust encryption which may be computationally intensive. However the size of the message is small and the transaction is a one time thing which is done at startup. The complexity of this encryption allows for a very high level of security. Since this encryption and decryption take place infrequently, preferably only at startup, there is very little penalty to taking some time. A typical user will not mind and may not even notice a delay of up to even a few

seconds during the initiation or loading of a media title. One preferred sequence of events in just one preferred embodiment is as follows.

The primary information is MPEG encoded data. The main channel (not shown - part of information stream 12) from the DVD media 11 contains MPEG encoded data. The DVD version of MPEG contains multiple opportunities for scrambling. Scrambling bits are defined and/or reserved bits exist in Video, Audio, Sub-picture, Data Search Information, and Video Blanking Information packs.

The copy protection method described here scrambles the video and/or audio and/or sub pictures. An encoded version of the scrambling control bits are then inserted into the MPEG stream. Direct de-scrambling based on the inserted scrambling control bits will not give the correct results. To obtain correct de-scrambling, the scrambling control bit stream must be processed through a decoder, such as a tapped shift register.

The primary information key includes information on the correct setup of the decoder, such as position of the taps for correct scrambling control bit decoding. This primary information key is put on the media in a sub channel or an area that is addressable by physical address, but not by logical block address.

This last requirement means the drive controller can access the information needed for decoding scrambling control, but the host system 16 cannot obtain it by a read command to a logical block address. The drive controller 13 is designed to pass this information over to the host system 16 only in encrypted form using the controller's private key and the public key of the intended recipient. In Figure 1 the intended recipient is the MPEG decoder 40, particularly the descrambling unit illustrated by its buffer area 41.

The recipient, MPEG decoder 40, uses its private key and the controller's public key to decrypt the information that originated in the media sub channel or logically unaddressable regions.

If the scrambled MPEG data stream 12 is directed to a recording device, the copy protection scheme is not defeated because the information to properly decode the scrambling control bits is not present in any form. The required information passes through the host in encrypted form only and is therefore useless even if trapped and recorded.

The operating system brokers the exchange of public keys between the controller and the MPEG decoder at startup.

At startup, the DVD-ROM device driver (not shown, part of system software) requests the operating system to provide the public keys of any

installed MPEG2 decoders. The operating system obtains public keys from drive 10 and MPEG2 decoder 40 (if present). The operating system provides the public key of the decoder 40 to the drive 10 and public key of the drive 10 to the decoder 40. The DVD-ROM device driver refuses to accept any MPEG decoder public key except during the startup sequence. This give some extra security against impersonation.

Use of the Primary Information Key

During primary data transfer operation, the primary information key is used by the recipient, e.g. the MPEG decoder, to correctly reorder the scrambled logical blocks received by streaming off of the storage device, e.g. a DVD disk. The specific function of the primary information key depends on the specific scrambling scheme. One preferred scrambling scheme is described below. Once transferred to the recipient, the primary information key is inserted into an appropriate decoder, then used to unscramble the primary data stream. In a preferred embodiment, the primary data stream is scrambled MPEG data which is descrambled to give a traditional MPEG data stream which then is decoded to give a video image, for example, an NTSC standard image or an RGB image, which can be displayed on an appropriate monitor.

Scrambling Scheme

The preferred scrambling scheme is designed to be computationally intensive to break if attacked as a jig saw puzzle, but easy to reorder if the key is available. A data unit is divided into smaller units, which are then rearranged according to a selected scheme. Information for reordering that data unit is stored for retrieval in conjunction with that data unit. This might take the form of a scrambling vector, which might be stored in a subheader or perhaps embedded in the scrambled data unit. The information can be further protected by encoding the scrambling vector according to an encryption scheme, using a selected primary information key. The same process can be repeated for subsequent data units, but each data unit can be rearranged in a different order. In each instance, the scrambling vector is retrievable and can be reassociated with its corresponding data unit. The same primary information key can be used to encode a series of scrambling vectors. The primary information key, along with each particular instance of the encoded

scrambling vector, is used to decode the scrambling vector which in turn is used to correctly reorder the data unit.

In one particularly preferred embodiment, a selected program, such as a movie title, is divided into data units, each of which is scrambled individually, and each scrambling vector is encoded using a single key. That primary information key can be stored with the primary program, and each program can use a different primary information key. The specific scrambling and descrambling schemes can be implemented in specialized hardware for rapid and convenient playback of the primary program.

Figures 2A, 2B, 2C, 3 and 4 describe one scrambling embodiment that uses a scrambling vector subheader on 2 KB data blocks. If the user data stream (information or primary data stream) has places to put this scrambling vector data, it could be placed inside the user data and no subheader would be necessary.

Referring to Figures 2A, 2B and 2C, Figure 2A illustrates representative, primary data as formatted and addressed before scrambling. The data to scramble is segmented into groups of 32 sequential blocks, also referred to as sectors, each having a logical block address (LBA), each containing 2 KB for a total of 64 KB. Data in this form is considered clear text. For example, if it were MPEG2 movie data, it would be directly decodable by an MPEG2 decoder conforming to the published standards.

Changing the order of the sequential blocks scrambles the primary information. Figure 2B illustrates data as formatted and addressed after scrambling of LBAs and user data blocks in the 64 KB sequence. There are 32! distinct ways to randomly assign the data blocks to the 32 LBAs in each 64 KB sequence. The illustrated order, 5, 31, 17, ..., 22, is merely illustrative. Each group of 32 sectors can be scrambled independently and the correct position within the group given by the value of the Scrambling Vector Element (SVE) placed in a subheader.

Figure 2C illustrates data as formatted and addressed after scrambling of LBAs and user data blocks in the 64 KB segment. The scrambled form, SV*, of the scrambling vector, SV, is now placed in the subheaders of the group of 32 sectors. The SV*E user data are mastered onto the media, such as a DVD disc, in the sequence shown in Figure 2C. If the data stream is a scrambled MPEG2 movie, a standard MPEG2 decoder will not be able to make any sense out of it in the scrambled form.

Referring to Figure 3, this figure shows encryption of a 32 element scrambling vector. The elements of the scrambling vector are encrypted using a

reversible algorithm whose parameters are defined by the media key, K_{Media}. Recall this is the key that is only readable by the drive 10, and this key is never passed as clear text through the open system. There are a number of simple approaches available for encrypting the scrambling vector, such as tapped shift registers, pseudo random sequence generators, etc.

Referring to Figure 4, descrambling is done inside MPEG2 decoder 40. The descrambling buffer area 41 is equal to or greater than the 64 KB of user data plus the 32 byte overhead of the SV*. Typical memory allocation might be done on 1 KB boundaries, so handling the SV* and converting it back to SV might necessitate 65 KB for the descrambling buffer area. The internal output is a clear text MPEG data stream which is then decoded to give final output 19 as uncompressed video.

Other data streams can be processed in an analogous manner.

Another preferred scrambling scheme reorders only part of the user data block. An MPEG data stream includes high order bits that define information about the sequence of the user data blocks. If data blocks including this information were simply reordered, it would be possible to use those specific bits to reassemble the data in the correct order. However, if only part of the user block is reordered and the expected sequence information is left untouched, the user blocks will be corrupted because the first part of the user block will be matched with the second part of a different user block. In a preferred implementation, the first half of each block is untouched while the second half of each block is reordered as described above in connection with Figures 2A, 2B and 2C. The scrambling vector is prepared, encoded and stored as described above. This scheme still has 32! possible combinations. Since each data unit can be reordered using a different scrambling vector, descrambling will be difficult without the key, but simple with the correct primary information key.

The size of the data unit affects the complexity of encoding and decoding. The example above describes a data unit subdivided into 32 blocks. This allows reordering in 32! possible combinations which gives a fairly complex, and thus secure, encoding scheme. In the DVD specification, a standard data unit is 32 KB of 2 KB subunits. This provides 16 blocks which can be reordered as decribed above, to give 16! possible combinations of scrambled data.

A media drive controller can be designed to support this scheme at minimal cost impact. As far as the transferring a scrambled primary data stream, a traditional drive controller need not be modified at all. To support

the secondary encoding, the drive controller needs to maintain a public and a private key had be able to support the selected encryption scheme. To support the preferred embodiment of storing the primary information key in a special location on the media, the drive controller needs to be designed to achieve the needed access and transfer the key appropriately.

The recipient similarly may need only minor modification. If the data stream decoder is a separate unit, there may be no need to modify the decoder. In a preferred embodiment, the recipient is or is coupled to a descrambler unit which in turn is tightly coupled to a decoder such as an MPEG decoder. The descrambler unit should support the selected scrambling scheme and should manage the primary information key as needed. In a preferred embodiment, the descrambler manages a public and a private key, interfacing with the secure data channel, receiving and decrypting the primary information key, and using the primary information key to descramble the primary information.

A general description of the device and method of using the present invention as well as a preferred embodiment of the present invention has been set forth above. One skilled in the art will recognize and be able to practice many changes in many aspects of the device and method described above, including variations which fall within the teachings of this invention. The spirit and scope of the invention should be limited only as set forth in the claims which follow.

Claims

What is claimed is:

1. An apparatus for providing two levels of copy protection, said apparatus comprising

first means for copy protecting information, said first means including a key, and

second means for copy protecting information, said second means applied to said key for said first means.

2. The apparatus of claim 1 wherein said first means for copy protecting information is a selective disordering of an information data stream and said key can be used to correctly reorder the disordered information data stream.

3. The apparatus of claim 1 further comprising two devices connected by a communication channel and wherein said second means for copy protecting information is a means to provide a secure communication channel between two devices.

4. The apparatus of claim 3 wherein said second means for copy protecting information includes use of a public and private key by at least one of said two devices.

5. The apparatus of claim 3 wherein said key for said first means for copy protecting information is encoded for transmission over said communication channel between said two devices.

6. The apparatus of claim 1 further comprising

a source of information encoded according to a first means for copy protection,

a decoder for said information according to said first means for copy protection, using said key,

a storage location for said key,

a means for communicating between said storage location and said decoder,

wherein said second means for copy protecting information comprises means for encoding said key for secure communication between said storage location and said decoder.

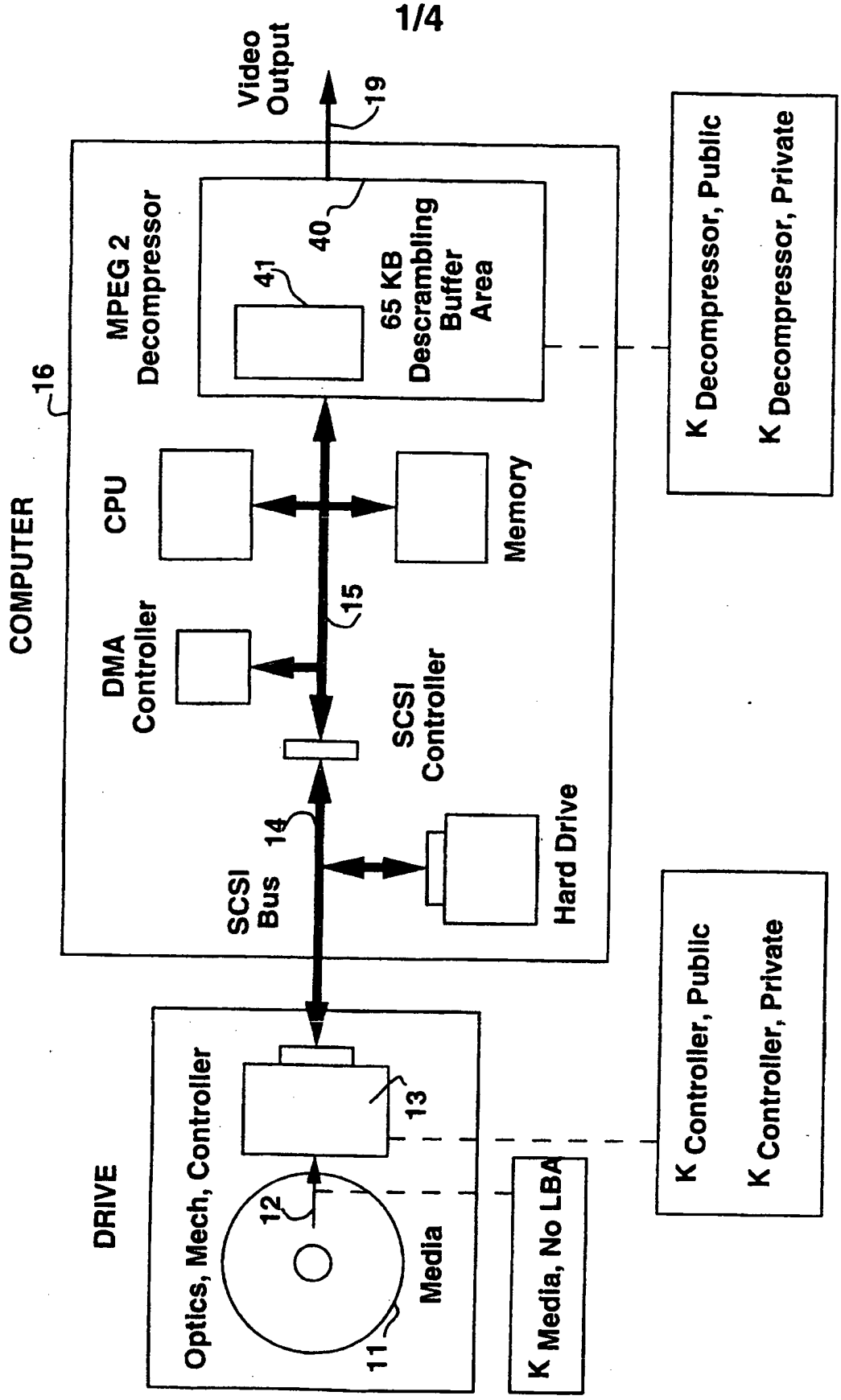

Video Output
19
MPEG 2 Decompressor
40
41
65 KB Descrambling Buffer Area
K Decompressor, Public
K Decompressor, Private
COMPUTER
16
CPU
Memory
DMA Controller
15
SCSI Controller
SCSI Bus
14
Hard Drive
DRIVE
Optics, Mech, Controller
13
12
Media
11
K Media, No LBA
K Controller, Public
K Controller, Private

Figure 1

LBA n	2 KB User Data (block n)
LBA n + 1	2 KB User Data (block n + 1)
LBA n + 2	2 KB User Data (block n + 2)
LBA n + 3	2 KB User Data (block n + 3)
LBA n + 4	2 KB User Data (block n + 4)
LBA n + 5	2 KB User Data (block n + 5)
LBA n + 31	2 KB User Data (block n + 31)

FIGURE 2A

LBA n	SVE 0 (5)	2 KB User Data (block n + 5)
LBA n + 1	SVE 1 (31)	2 KB User Data (block n + 31)
LBA n + 2	SVE 2 (17)	2 KB User Data (block n + 17)
LBA n + 3	SVE 3 (4)	2 KB User Data (block n + 4)
LBA n + 4	SVE 4 (24)	2 KB User Data (block n + 24)
LBA n + 5	SVE 5 (0)	2 KB User Data (block n)
.....	.....	.....
.....	.....	.....
LBA n + 31	SVE 31 (22)	2 KB User Data (block n + 22)

FIGURE 2B

LBA n	SV* E 0	2 KB User Data (block n + 5)
LBA n + 1	SV* E 1	2 KB User Data (block n + 31)
LBA n + 2	SV* E 2	2 KB User Data (block n + 17)
LBA n + 3	SV* E 3	2 KB User Data (block n + 4)
LBA n + 4	SV* E 4	2 KB User Data (block n + 24)
LBA n + 5	SV* E 5	2 KB User Data (block n)
.....	.....	.....
.....	.....	.....
LBA n + 31	SV* E 31	2 KB User Data (block n + 22)

FIGURE 2C

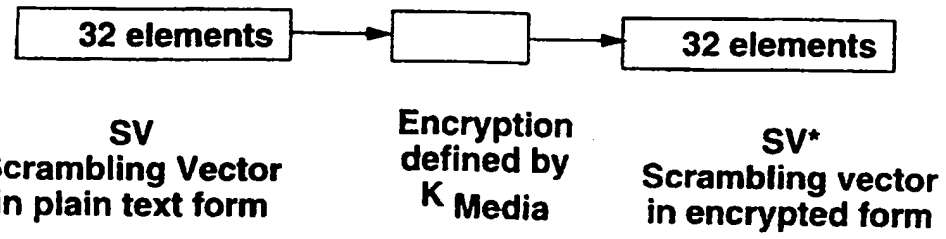


FIGURE 3

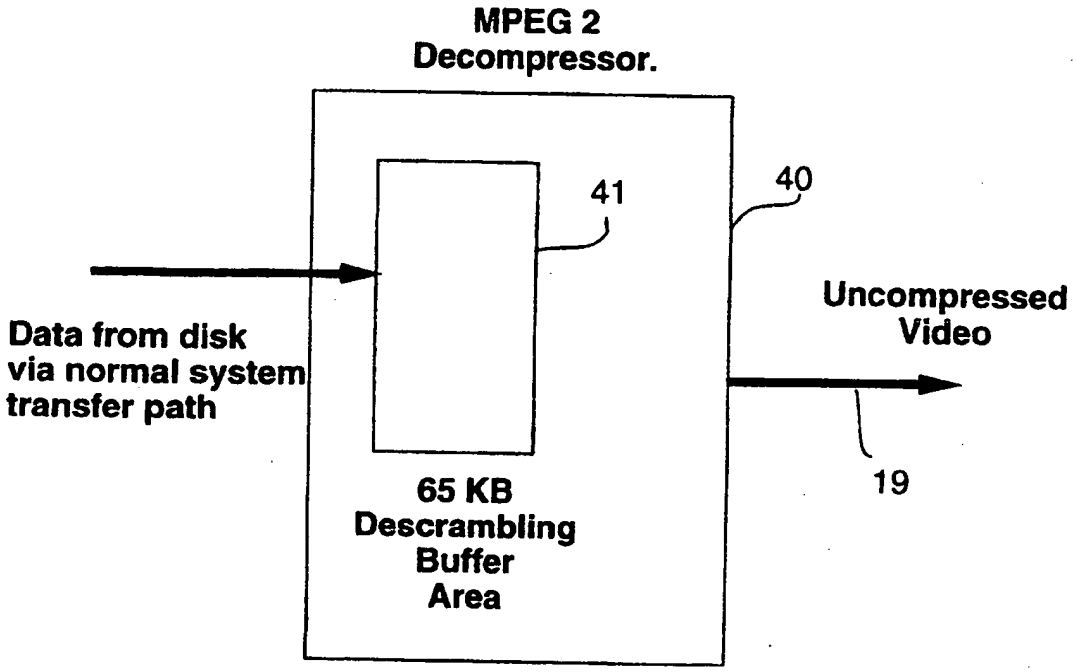


FIGURE 4

INTERNATIONAL SEARCH REPORT

Interna al Application No
PCT/US 97/08264

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06F12/14

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G06F G11B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 058 162 A (SANTON JOHN C ET AL) 15 October 1991 see abstract; figures 2,6,7 see column 2, line 24 - line 31 see column 3, line 4 - line 19 see column 7, line 20 - line 49 ---	1,3,5,6
X	US 4 903 296 A (CHANDRA AKHILESHWARI N ET AL) 20 February 1990 see abstract; figures 1,7.1 see column 3, line 2 - column 4, line 31 see column 7, line 22 - line 61 see column 8, line 37 - column 9, line 2 ---	1,3-6
A	US 5 438 622 A (NORMILE JAMES O ET AL) 1 August 1995 cited in the application see the whole document ---	1,3-6
	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

1

Date of the actual completion of the international search	Date of mailing of the international search report
9 October 1997	13.10.97

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Powell, D

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Internat' l Application No
PCT/US 97/08264

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 319 705 A (HALTER BERNARD J ET AL) 7 June 1994 see column 3, line 17 - line 29 ---	2
A	US 4 168 396 A (BEST ROBERT M) 18 September 1979 see abstract; figures 1,2 see column 3, line 60 - column 4, line 48 ---	2
A	US 5 224 166 A (HARTMAN JR ROBERT C) 29 June 1993 -----	

1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Interna al Application No
PCT/US 97/08264

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5058162 A	15-10-91	JP 5173891 A	13-07-93
US 4903296 A	20-02-90	US 4644493 A	17-02-87
		DE 3587658 D	23-12-93
		DE 3587658 T	11-05-94
		EP 0174472 A	19-03-86
		JP 1650990 C	30-03-92
		JP 3012744 B	20-02-91
		JP 61072345 A	14-04-86
US 5438622 A	01-08-95	NONE	
US 5319705 A	07-06-94	JP 7093148 A	07-04-95
US 4168396 A	18-09-79	US 4278837 A	14-07-81
US 5224166 A	29-06-93	EP 0583140 A	16-02-94
		JP 2085066 C	23-08-96
		JP 6112937 A	22-04-94
		JP 7107989 B	15-11-95